Per eseguire l'esercizio di scansione dell'host utilizzando Nmap con diversi comandi e opzioni, seguirò le istruzioni fornite. Ogni comando sarà eseguito sulla macchina Metasploitable (ip address: 192.168.3.245) e i risultati saranno riportati in un report dettagliato.

## Report di Scansione Utilizzando Nmap

### 1. Scansione TCP Completa

```
bash
nmap -sS 192.168.3.245
```

**Risultato:**

- Identifica le porte aperte e i servizi in esecuzione sulla macchina Metasploitable.

### 2. Scansione TCP e output su file

```
bash
nmap -sV -oN scan_results.txt 192.168.3.245
```

**Risultato:**

- Esegue una scansione TCP con rilevamento delle versioni dei servizi e salva i risultati in un file di testo (`scan_results.txt`).

### 3. Scansione su una porta specifica (8080)

```
bash
nmap -sS -p 8080 192.168.3.245
```

**Risultato:**

- Scansiona la porta 8080 utilizzando la scansione SYN.

### 4. Scansione su tutte le porte TCP

```
bash
nmap -sS -p- 192.168.3.245
```

**Risultato:**

- Scansiona tutte le porte TCP sulla macchina Metasploitable.

### 5. Scansione UDP

```
bash
nmap -sU -r -v 192.168.3.245
```

**Risultato:**

- Esegue una scansione UDP utilizzando un'approccio aggressivo per rilevare i servizi UDP aperti.

### 6. Scansione del Sistema Operativo

```
bash
nmap -O 192.168.3.245
```

**Risultato:**

- Tentativo di identificare il sistema operativo in esecuzione sulla macchina Metasploitable.

### 7. Scansione Versione Servizi

```
bash
nmap -sV 192.168.3.245
```

**Risultato:**

- Identifica le versioni dei servizi aperti sulla macchina Metasploitable.

### 8. Scansione delle 100 porte comuni

```
bash
nmap -F 192.168.3.245
```

**Risultato:**

- Esegue una scansione rapida sulle 100 porte TCP più comuni.

### 9. Scansione tramite ARP

```
bash
nmap -PR 192.168.3.245
```

**Risultato:**

- Esegue una scansione ARP per scoprire i dispositivi nella stessa subnet.

### 10. Scansione tramite PING

```
bash
nmap -sP 192.168.3.245
```

**Risultato:**

- Esegue una scansione utilizzando il protocollo ICMP per scoprire i dispositivi attivi (con PING).

### 11. Scansione senza PING

```
bash
nmap -PN 192.168.3.245
```

**Risultato:**

- Esegue una scansione senza inviare PING, per determinare lo stato delle porte aperte senza considerare la risposta al PING.

## Conclusione

Nmap è uno strumento potente per la scansione di host e reti, fornendo una vasta gamma di opzioni per l'identificazione di porte aperte, servizi in esecuzione, sistema operativo e altro ancora. Le informazioni raccolte durante la scansione sono fondamentali per comprendere il paesaggio di sicurezza di un sistema e per identificare eventuali vulnerabilità che potrebbero essere sfruttate.